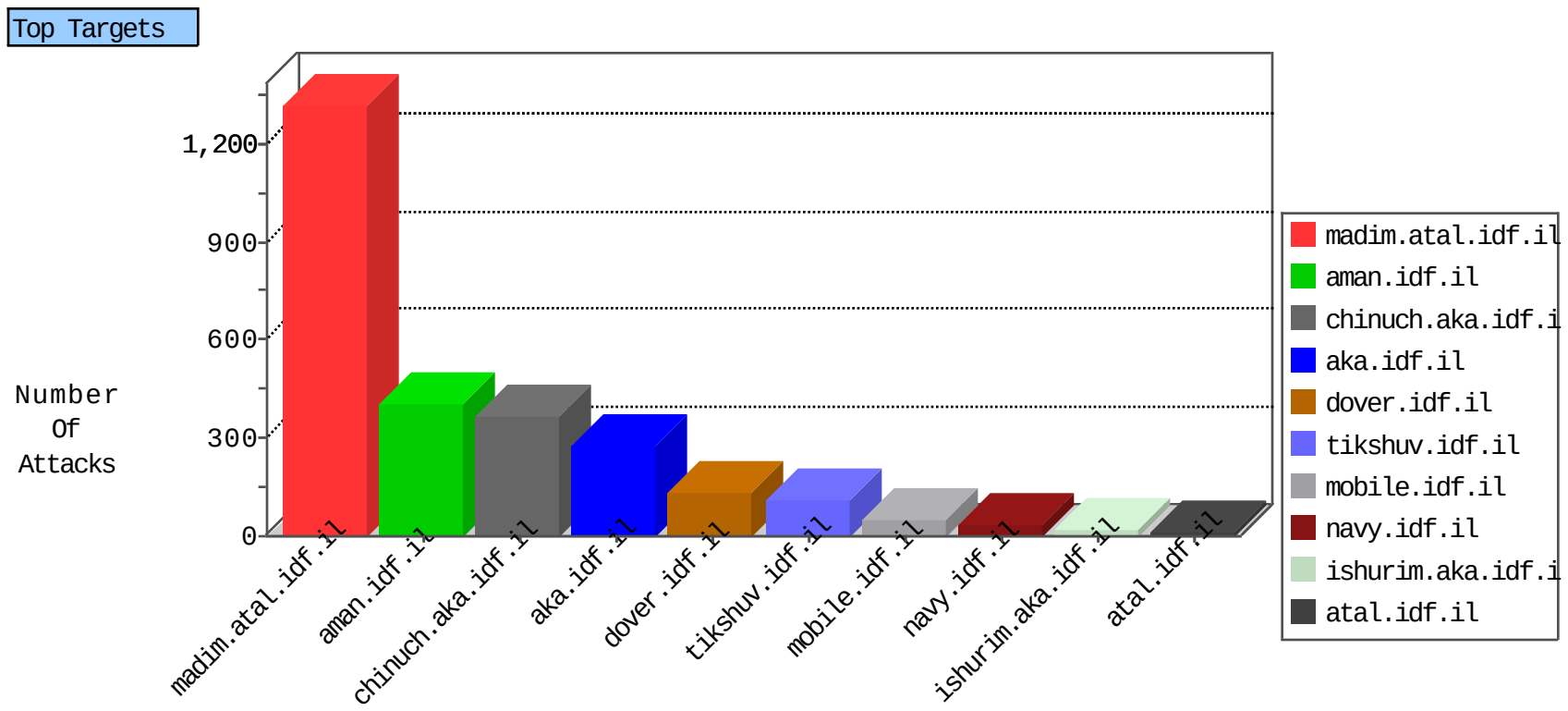
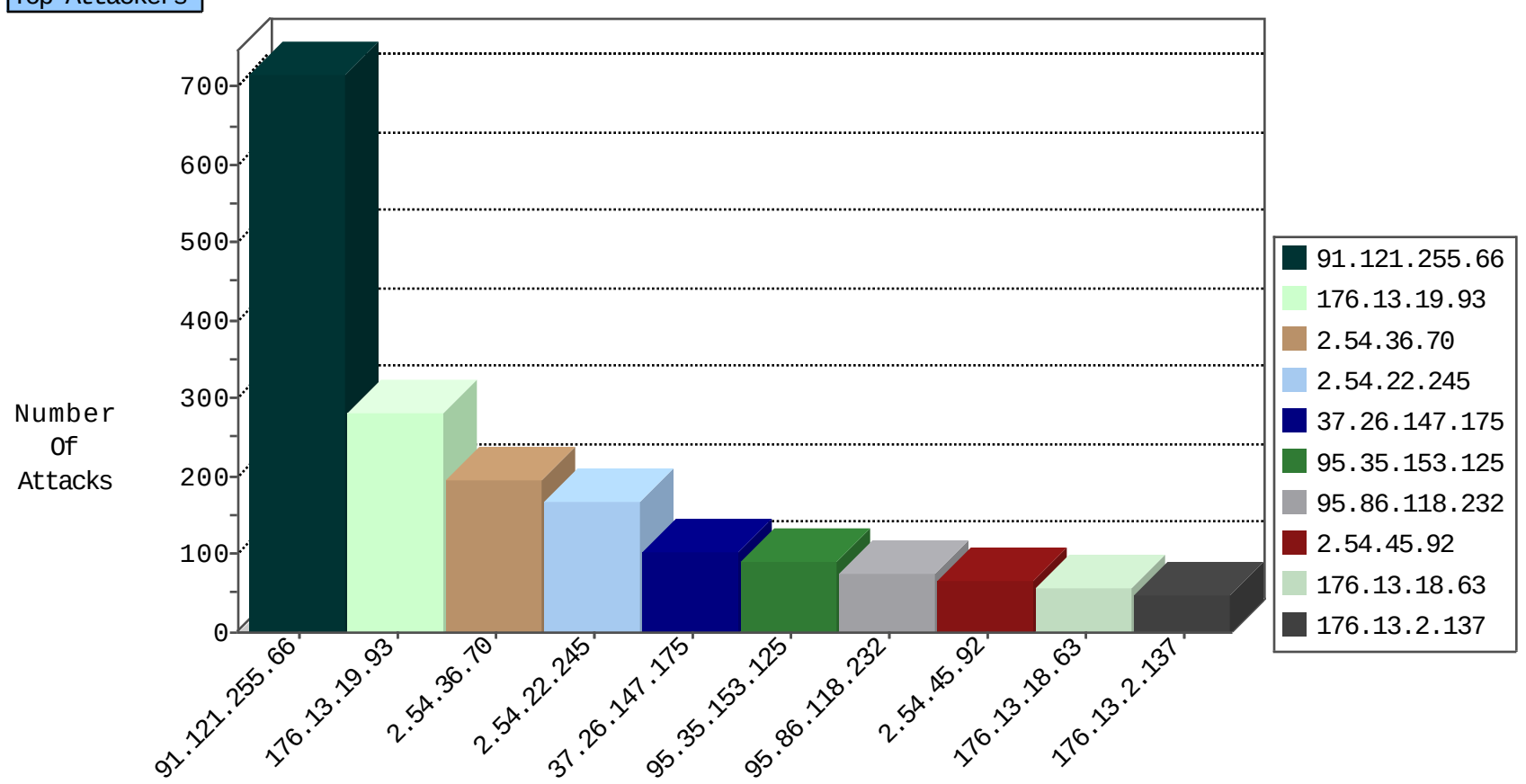
01-26-2016-13:04:09 to 01-26-2016-14:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-26-2016-13:04:09 to 01-26-2016-14:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
108.17.85.141	United States	147.237.72.156	aman.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
142.54.169.166	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1

01-26-2016-13:04:09 to 01-26-2016-14:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.75	France	147.237.0.15	kosher-kravi.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-26-2016-13:04:09 to 01-26-2016-14:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
90.194.241.234	147.237.72.166	United Kingdom	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
84.95.45.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.29.203.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.175.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.42	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.19.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
108.17.85.141	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
108.17.85.141	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.130	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.237.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.96.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.95.33	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
46.117.184.73	147.237.72.156	Israel	aman.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.127	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.7.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
108.17.85.141	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
95.86.115.166	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

01-26-2016-13:04:09 to 01-26-2016-14:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	339
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	335
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.i	SYN Attack		reject	20
2.54.59.41	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack		reject	13
46.19.86.65	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.67.208.45	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.141.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.64.50.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	7
46.19.86.56	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.70	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.5.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.5.96	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.54.41.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.90.139.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.102.254.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.51.218	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.178	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.250.187.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.59.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
132.70.66.12	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
188.120.148.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
80.179.98.55	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.14.114	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.104	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.179.98.55	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.204.128.94	Netherlands	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
82.81.14.58	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
189.253.17.67	Mexico	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.59.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.186.110	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.183.28.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.136.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.122.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.230	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.133.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
86.58.78.193	Slovenia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.162.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.128	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	174
176.13.19.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	108
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
2.54.36.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	97
2.54.36.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	92
95.35.153.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
95.86.118.232	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	76
37.26.147.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
2.54.45.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
176.13.18.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
176.13.2.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
2.54.154.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
2.54.182.221	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	40
79.180.101.114	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
46.19.85.119	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
176.13.19.106	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
176.13.9.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
37.26.147.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	27
2.54.22.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	24
46.117.88.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	15
46.19.86.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
80.246.138.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
46.19.85.92	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
95.86.67.126	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 95.86.67.126	Block	10
80.246.137.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.160.233.66	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.160.233.66	Block	7
46.19.86.227	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	4
79.182.96.48	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	4
2.52.15.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.210.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.59.65	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.136.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.156.144	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.65	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.128.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.193.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.131.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
213.151.35.213	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.137.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.146.201	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.12.122	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.160.233.66	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2

01-26-2016-13:04:09 to 01-26-2016-14:04:09